UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/887,585	06/21/2001	David W. Carman	NA01-00201	8239

28875	7590	05/24/2005

Zilka-Kotab, PC
P.O. BOX 721120
SAN JOSE, CA 95172-1120

EXAMINER
LANIER, BENJAMIN E

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 05/24/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) FROM
THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
  after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
  earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>08 April 2005</u>.

2a)☒ This action is **FINAL**.   2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is
   closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) <u>1-39</u> is/are pending in the application.

   4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) <u>1-39</u> is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on <u>21 June 2001</u> is/are: a)☒ accepted or b)☐ objected to by the Examiner.

   Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

   Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

   a)☐ All   b)☐ Some * c)☐ None of:

   1.☐ Certified copies of the priority documents have been received.

   2.☐ Certified copies of the priority documents have been received in Application No. _____.

   3.☐ Copies of the certified copies of the priority documents have been received in this National Stage
      application from the International Bureau (PCT Rule 17.2(a)).

   * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☐ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
   Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413)
   Paper No(s)/Mail Date. _____.

5)☐ Notice of Informal Patent Application (PTO-152)

6)☐ Other: _____.

DETAILED ACTION

Response to Amendment

1.   Applicant's amendment filed 08 April 2005 amends claims 1, 5, 19, 37. Applicants

amendment has been fully considered and is entered.

Response to Arguments

2.   Applicant's arguments filed 08 April 2005 have been fully considered but they are not

persuasive. Applicant's argument that it would have been unobvious to combine the teachings of

Mizikovsky with the teachings of Tatebayashi because Tatebayashi discloses that the

cryptographic key is generated at the network center is not persuasive because Mizikovsky

discloses that the cryptographic key is generated at the base station and the wireless terminals.

Mizikovsky removes the necessity of transmitting the generated key from the network

center/base station to the wireless terminals, which is beneficial because Mizikovsky discloses

that it is unwise to transmit a secret key over a wireless channel (Col. 1, lines 65-66). Therefore,

improving the key distribution protocol of Tatebayashi with the teachings of Mizikovsky would

have been obvious to one of ordinary skill in the art at the time the invention was made in order

to enhance the security of wireless communication infrastructure as taught in Mizikovsky (Col.

8, lines 14-19) by not having the secret keys transmitted over the air.

3.   Applicant's argument that there is no showing in the prior art of energy usage being

shifted to a super node by performing private key decryption at the super node is not persuasive

because Tatebayashi discloses that the network center performs the private key decryption

(Section 3), which would meet the above mentioned limitation because Applicant contends that

encrypting with a public key requires less energy than decrypting with a private key. Therefore,

the protocol described in Tatebayashi effectively shifts the energy usage to the network center as claimed by Applicant.

4.   Applicant's assumption that the Examiner relies solely on Mizikovsky (Col. 7, lines 9-65) to meet the limitations of claim 4 is incorrect because "sending a third message from the second node to the super node wherein the third messages includes the second partial key value encrypted using the public key belonging to the super node, recovering the second partial key value at the super node by decrypting using the private key" is meet by Tatebayashi (Section 3) where the second terminal generates a second-key-encryption-key signal and encrypts this signal using the public key of the network center. The encrypted second-key-encryption key is transmitted to the network center and decrypted with the private key of the network center. The limitation of "securely communicating the second partial key value to the first node and establishing the cryptographic key at the first node using the first partial key value and the second partial key value" is meet by Mizikovsky (Col. 7, lines 9-65), which teaches the base station transmits the seed of a second wireless terminal to the first wireless terminal in order for the first wireless terminal to generate the cryptographic key. The motivation to combine the references is explained above and provided below in the rejection.

Claim Rejections - 35 USC § 103

5.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. The factual inquiries set forth in *Graham* v. *John Deere Co.*, 383 U.S. 1, 148 USPQ 459

(1966), that are applied for establishing a background for determining obviousness under 35

U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

7. Claims 1, 4, 7, 10, 11, 14, 19, 22, 25, 28, 29, 32 are rejected under 35 U.S.C. 103(a) as

being unpatentable over Tatebayashi, in view of Mizikovsky, U.S. Patent No. 5,748,734.

Referring to claims 1, 4, 19, 22, Tatebayashi discloses a key distribution protocol wherein when

a first user at a first terminal desires to share a common key or secret key with a second user at a

second terminal, the first user generates a random number as a first key encryption key. The first

key encryption key signal is passed to the network center using a public key scheme (Section 3),

which meets the limitation of sending a first message from the first node to the super node,

wherein the first message includes a first partial key value encrypted using a public key

belonging to the super node, whereby encrypting with the public key requires less energy than

decrypting with a private key corresponding to the public key. The network center receives the

key encryption key (Section 3), which meets the limitation of recovering the first partial key

value at the super node by decrypting using the private key. Tatebayashi does not disclose that

the network center transmits the key encryption key of the first node to the second node, the key

encryption key of the second node to the first node, or establishing the common or secret key for

communication between the first node and the second node by the first and second nodes using

the received partial keys. Mizikovsky discloses a method of generating cryptographic keys for

communication between a first node and a second node wherein the first and second nodes

generate random seeds that are communicated through a base station to the other node. Once the

random seed of the other node is received a common cryptographic key is generated and used for

communication (Col. 7, lines 9-65), which meets the limitation of securely communicating the

first partial key value to the second node, establishing the cryptographic key at the second node

using the first partial key value and a second partial key value created by the second node,

sending a third message from the second node to the super node, wherein the third message

includes the second partial key value encrypted using the public key belonging to the super node,

recovering the second partial key value at the super node by decrypting using the private key,

securely communicating partial key value to the first node, and establishing the cryptographic

key at the first node using the first partial key value and the second partial key value. It would

have been obvious to one of ordinary skill in the art at the time the invention was made to the

generate the common cryptographic key of Tatebayashi in the nodes as well as the network

center in order to enhance the security of wireless communication infrastructure as taught in

Mizikovsky (Col. 8, lines 14-19).

Referring to claims 7, 10, 11, 14, 25, 28, 29, 32, Mizikovsky discloses that central facility

or network center stores the private keys for all users in a classic key system (Section 2.1), which

meets the limitation of encrypting communications from the super node to a selected node using

the symmetric key of that selected node.

8.   Claims 8, 9, 12, 13, 17, 18, 26, 27, 30, 31, 35, 36 are rejected under 35 U.S.C. 103(a) as

being unpatentable over Tatebayashi, in view of Mizikovsky, U.S. Patent No. 5,748,734 as

applied to claims 1, 4, 7, 11 above, and further in view of Menezes. Referring to claims 8, 12, 17,

18, 26, 30, 35, 36, Tatebayashi discloses a key distribution protocol wherein when a first user at

a first terminal desires to share a common key or secret key with a second user at a second

terminal, the first user generates a random number as a first key encryption key. The first key

encryption key signal is passed to the network center using a public key scheme (Section 3),

which meets the limitation of sending a first message from the first node to the super node,

wherein the first message includes a first partial key value encrypted using a public key

belonging to the super node, whereby encrypting with the public key requires less energy than

decrypting with a private key corresponding to the public key. The network center receives the

key encryption key (Section 3), which meets the limitation of recovering the first partial key

value at the super node by decrypting using the private key. Mizikovsky discloses a method of

generating cryptographic keys for communication between a first node and a second node

wherein the first and second nodes generate random seeds that are communicated through a base

station to the other node. Once the random seed of the other node is received a common

cryptographic key is generated and used for communication (Col. 7, lines 9-65), which meets the

limitation of securely communicating the first partial key value to the second node, establishing

the cryptographic key at the second node using the first partial key value and a second partial key

value created by the second node, sending a third message from the second node to the super

node, wherein the third message includes the second partial key value encrypted using the public

key belonging to the super node, recovering the second partial key value at the super node by

decrypting using the private key, securely communicating partial key value to the first node, and

establishing the cryptographic key at the first node using the first partial key value and the

second partial key value. Mizikovsky does not disclose the use of certificates to validate the keys

used during the communication process. Menezes discloses methods of key distribution and key

management wherein the symmetric keys used to set up secure communications are validated

using certificates (Pages 554-555). It would have been obvious to one of ordinary skill in the art

at the time the invention was made to validate the symmetric keys of Mizikovsky in order to

avoid the requirement of either user terminal or node maintaining a secure database of user

secrets as taught in Menezes (Page 554).

Referring to claims 9, 13, 27, 31, Menezes discloses that the certificates have a period of

validity that would require the acquisition of new symmetric keys (Page 554), which meets the

limitation of the certificate includes validation information for a plurality of symmetric keys and

wherein a new second node symmetric key is selected periodically from the plurality of

symmetric keys. It would have been obvious to one of ordinary skill in the art at the time the

invention was made to validate the symmetric keys of Mizikovsky in order to avoid the

requirement of either user terminal or node maintaining a secure database of user secrets as

taught in Menezes (Page 554).

9.   Claims 2, 3, 5, 6, 15, 16, 20, 21, 23, 24, 33, 34, 37, 38 are rejected under 35

U.S.C. 103(a) as being unpatentable over Tatebayashi, in view of Mizikovsky, U.S. Patent No.

5,748,734 as applied to claims 1, 4 above, and further in view of Menezes. Referring to claims 2,

3, 5, 6, 15, 16, 20, 21, 23, 24, 33, 34, 37, 38, Tatebayashi discloses a key distribution protocol

wherein when a first user at a first terminal desires to share a common key or secret key with a

second user at a second terminal, the first user generates a random number as a first key

encryption key. The first key encryption key signal is passed to the network center using a public

key scheme (Section 3), which meets the limitation of sending a first message from the first node

to the super node, wherein the first message includes a first partial key value encrypted using a public key belonging to the super node, whereby encrypting with the public key requires less energy than decrypting with a private key corresponding to the public key. The network center receives the key encryption key (Section 3), which meets the limitation of recovering the first partial key value at the super node by decrypting using the private key. Mizikovsky discloses a method of generating cryptographic keys for communication between a first node and a second node wherein the first and second nodes generate random seeds that are communicated through a base station to the other node. Once the random seed of the other node is received a common cryptographic key is generated and used for communication (Col. 7, lines 9-65), which meets the limitation of securely communicating the first partial key value to the second node, establishing the cryptographic key at the second node using the first partial key value and a second partial key value created by the second node, sending a third message from the second node to the super node, wherein the third message includes the second partial key value encrypted using the public key belonging to the super node, recovering the second partial key value at the super node by decrypting using the private key, securely communicating partial key value to the first node, and establishing the cryptographic key at the first node using the first partial key value and the second partial key value. Mizikovsky discloses that use of verification information that is transferred between the wireless terminals to authenticate the key transmissions (Col. 7, line 58 – Col. 8, line 14), but does not disclose that the verification information is a hash or a MAC. Menezes discloses that MACs are used for data verification (Page 362). It would have been obvious to one of ordinary skill in the art at the time the invention was made to use MAC codes

in the key distribution protocol of Tatebayashi in order to provide transaction authentication of exchanges between parties as taught in Menezes.

10.   Claim 39 is rejected under 35 U.S.C. 103(a) as being unpatentable over Tatebayashi, in view of Mizikovsky, U.S. Patent No. 5,748,734 and further in view of Menezes. Referring to claim 39, Tatebayashi discloses a key distribution protocol wherein when a first user at a first terminal desires to share a common key or secret key with a second user at a second terminal, the first user generates a random number as a first key encryption key. The first key encryption key signal is passed to the network center using a public key scheme (Section 3), which meets the limitation of sending a first message from the first node to the super node, wherein the first message includes a first partial key value encrypted using a public key belonging to the super node, whereby encrypting with the public key requires less energy than decrypting with a private key corresponding to the public key. The network center receives the key encryption key (Section 3), which meets the limitation of recovering the first partial key value at the super node by decrypting using the private key. Tatebayashi does not disclose that the network center transmits the key encryption key of the first node to the second node, the key encryption key of the second node to the first node, or establishing the common or secret key for communication between the first node and the second node by the first and second nodes using the received partial keys. Mizikovsky discloses a method of generating cryptographic keys for communication between a first node and a second node wherein the first and second nodes generate random seeds that are communicated through a base station to the other node. Once the random seed of the other node is received a common cryptographic key is generated and used for communication (Col. 7, lines 9-65), which meets the limitation of securely communicating the

first partial key value to the second node, establishing the cryptographic key at the second node

using the first partial key value and a second partial key value created by the second node,

sending a third message from the second node to the super node, wherein the third message

includes the second partial key value encrypted using the public key belonging to the super node,

recovering the second partial key value at the super node by decrypting using the private key,

securely communicating partial key value to the first node, and establishing the cryptographic

key at the first node using the first partial key value and the second partial key value. Mizikovsky

discloses that central facility or network center stores the private keys for all users in a classic

key system (Section 2.1), which meets the limitation of encrypting communications from the

super node to a selected node using the symmetric key of that selected node, wherein the first

and second node symmetric key is saved at the super node so that a subsequent key

establishment can use symmetric key encryption for encrypting the first partial key value. It

would have been obvious to one of ordinary skill in the art at the time the invention was made to

the generate the common cryptographic key of Tatebayashi in the nodes as well as the network

center in order to enhance the security of wireless communication infrastructure as taught in

Mizikovsky (Col. 8, lines 14-19). Mizikovsky discloses that use of verification information that

is transferred between the wireless terminals to authenticate the key transmissions (Col. 7, line

58 – Col. 8, line 14), but does not disclose that the verification information is a hash or a MAC.

Menezes discloses that MACs are used for data verification (Page 362), which meets the

limitation of a second message is sent from the first node to the second node, wherein the second

message includes a first message authentication code, wherein the first partial key value is

authenticated at the second node using the first message authentication code, wherein a fourth

message is sent from the second node to the first node, wherein the fourth message includes a

second message authentication code, wherein the second partial key value is authenticated at the

first node using the second message authentication code, establishing the cryptographic key at

the first and second nodes by hashing the first and second partial key values. It would have been

obvious to one of ordinary skill in the art at the time the invention was made to use MAC codes

in the key distribution protocol of Tatebayashi in order to provide transaction authentication of

exchanges between parties as taught in Menezes. Mizikovsky does not disclose the use of

certificates to validate the keys used during the communication process. Menezes discloses

methods of key distribution and key management wherein the symmetric keys used to set up

secure communications are validated using certificates (Pages 554-555), which meets the

limitation of trust of the super node is established at the first node and the second node by

validating a certificate provided by a recognized certificate authority and presented to the first

node and second node by the super node. It would have been obvious to one of ordinary skill in

the art at the time the invention was made to validate the symmetric keys of Mizikovsky in order

to avoid the requirement of either user terminal or node maintaining a secure database of user

secrets as taught in Menezes (Page 554). Menezes discloses that the certificates have a period of

validity that would require the acquisition of new symmetric keys (Page 554), which meets the

limitation of the certificate includes validation information for a plurality of symmetric keys and

wherein a new second node symmetric key is selected periodically from the plurality of

symmetric keys. It would have been obvious to one of ordinary skill in the art at the time the

invention was made to validate the symmetric keys of Mizikovsky in order to avoid the

requirement of either user terminal or node maintaining a secure database of user secrets as

taught in Menezes (Page 554).

Conclusion

11.   Applicant's amendment necessitated the new ground(s) of rejection presented in this

Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a).

Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE

MONTHS from the mailing date of this action. In the event a first reply is filed within TWO

MONTHS of the mailing date of this final action and the advisory action is not mailed until after

the end of the THREE-MONTH shortened statutory period, then the shortened statutory period

will expire on the date the advisory action is mailed, and any extension fee pursuant to 37

CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event,

however, will the statutory period for reply expire later than SIX MONTHS from the date of this

final action.

12.   Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Benjamin E. Lanier whose telephone number is 571-272-3805.

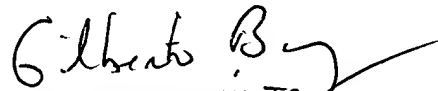The examiner can normally be reached on M-Th0 7:30am-5:00pm, F 7:30am-4pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the

organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent

Application Information Retrieval (PAIR) system. Status information for published applications

may be obtained from either Private PAIR or Public PAIR. Status information for unpublished

applications is available through Private PAIR only. For more information about the PAIR

system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR

system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Benjamin E. Lanier

GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100